

UNITED STATES V. ELLIOT DOXER

AGREED STATEMENT OF FACTS

On or about June 22, 2006, ELLIOT DOXER, an employee at the headquarters of Akamai Technologies, Inc. ("Akamai") in Cambridge, Massachusetts, sent an email to the Israeli Consulate in Boston, Massachusetts, containing the following message (with its original punctuation and capitalization):

I am a jewish american who lives in Boston. I know you are always looking for information and i am offering the little i may have.

I work in a high tech company called Akamai technologies and i work in the finance department.

we have more important clients including department of defense, airline manufacturers like Airbus and some Arab companies from Dubai. And today, Attorney General Alberto Gonzales is here on premises

I would be happy to provide information to you but the limit of my information is invoicing and customer contact information. All this may not be of any value to you but i would offer any help i can to help Israel.

Because Google, Inc., which maintains Gmail.com (the email service DOXER used), did not maintain any email servers in Massachusetts in June 2006, the email necessarily crossed state lines twice: when it traveled from DOXER's computer in Massachusetts to one of Google's out-of-state Gmail servers, and when it traveled from that server to the Israeli Consulate in

Boston.

Akamai maintains the largest distributed computer network in the world, with over 42,000 computer servers located in over 900 networks across over 70 countries. Akamai's network handles 15-30% of the world's Internet traffic every day.

Akamai specializes in Internet content delivery, which, in essence, consists of using Akamai's computer network to distribute its customers' Internet information for a fee.

Akamai's network can be used by the customer to distribute any portion of the customer's website, from individual objects on a given webpage, to a single webpage of the site, to the entire website. A business or organization that wants to present information over a website itself must usually invest in the necessary computer hardware, software, real estate, network bandwidth, and personnel to manage the website and information. Akamai's Internet content delivery customers, however, can reduce their costs by letting Akamai's content delivery network do the work for them. In addition, even if Akamai's customers manage their own websites, the customers can augment their capabilities with Akamai's services. For example, Akamai's network can speed up its customers' websites and help handle increased demand for their information.

On September 18, 2007, an FBI undercover agent ("UA") pretending to be an Israeli intelligence agent called DOXER at work and had the following conversation with him, which was

recorded:

UA: Elliot, my name is Benjamin.

DOXER: Yeah.

UA: I am calling because I believe that you and I, I understand that we share a mutual interest in the welfare of our people and our homeland.

DOXER: Okay.

UA: And, you may recall that you made an offer, an offer to help us about a year ago or so.

DOXER: Ah! Is this who I think it is?

UA: I think you know exactly who it is.

DOXER: Okay.

UA: The – it took us a little while, but, finally, we're getting in touch with you regarding that matter.

DOXER: Okay.

[Discussion of communications procedures]

DOXER: You know I mean, I don't have much to offer, but whatever, whatever I have, you know, I want to help. [Laughter.]

UA: Well look, look, you know it's like a jigsaw puzzle, sometimes the pieces of the puzzle, and they may to you seem insignificant –

DOXER: – okay –

UA: – but when I put the puzzle together, maybe they mean something.

DOXER: Okay.

[Discussion confirming that DOXER had not discussed his offer with anyone else, instructing him not to mention the phone call to anyone else, confirming that the agent

represented Israel, and summarizing the communications procedures.]

A new UA (who assumed the identity of the original one) established a spot where DOXER could leave and pick up written communications ("the dead drop") and mailed DOXER written instructions on how to use the dead drop. Over the course of the next 18 months, DOXER visited the dead drop on at least 62 occasions to place items, retrieve items, and/or check for new items. All of Doxer's visits to the dead drop were surreptitiously videotaped.

On or about October 26, 2007, Doxer left a letter at the dead drop. He wrote, among other things, that he worked in Akamai's credit and collections or finance department, for which he contacted clients located in the United States and a number of foreign countries, including Israel. He wrote that he had access to names, e-mails, addresses, invoices, and signed contracts for most, if not all, of Akamai's clients. He also broadly described Akamai's physical and computer security systems. In response to written questions from the UA, DOXER indicated that he could travel to Israel and support special and sensitive operations in his local area if needed. He wrote that he had contacted Israel because he knew that Israel was always looking for information and he wanted to help Israel against its enemies.

On a number of occasions between November 2007 and March 2009, DOXER left at the dead drop trade secret information

belonging to Akamai. For example, on or about November 27, 2007, Doxer placed at the dead drop a thirteen-page list identifying over 2,000 of Akamai's customers. On several other occasions, DOXER placed at the dead drop business contracts between Akamai and various of its customers that included such sensitive details as the customer's name and address; the customer contact's name, telephone number, and e-mail address; the term of the contract; the expiration date; the services provided; and prices. Doxer also placed at the dead drop contracts between Akamai and the FBI, the United States Department of Homeland Security, an aerospace company, and several Department of Defense contractors.

On or about December 26, 2007, DOXER left a letter at the dead drop in which he wrote, "You neglected to respond to my request for some kind of payment for my services. . . . I could be fired and am also breaking the law -- all I want is some compensation. What do you think is fair for the information I have provided? I think some of the things I have told you you would not be able to find out anywhere else[.]" On or about January 29, 2008, DOXER left another letter at the dead drop in which he wrote, "I haven't thought much about a fair price, but will let you know -- I am interested in helping Israel and money is not my primary motivation for helping you. A few thousand dollars is not unreasonable to me." DOXER went on to ask for a few thousand dollars and stated, "I am not motivated by money but

in my desire to help our homeland and our war against our enemies."

In sum, between approximately November 2007 and approximately March 2009, DOXER provided trade secret information belonging to Akamai to an individual he believed to be an Israeli intelligence agent. The information included an extensive list of Akamai's customers and business contracts and associated contractual documents between Akamai and over 20 Akamai customers. DOXER provided these documents to benefit the Government of Israel. At a later point, Doxer asked about the possibility of payment for the information he was providing.

Akamai employs more than 2,000 people (approximately 600 in Massachusetts), carries 15% to 30% of the world's web traffic every day, and posted an annual gross revenue of \$860 million in 2009. Despite Akamai's success in the content delivery network market, it competes against dozens of other providers, including at least one in Israel. To maintain its competitive edge, it keeps much of its customer and pricing information confidential.

The customer list Doxer provided the UC identified more than 2,000 Akamai customers, many of whose identities would not be readily ascertainable through proper means by the public. Those customers range in size from corporations that pay Akamai \$1 million or more per month to those that pay approximately \$2,000 - \$3,000 per month. Akamai keeps the identity of most of its

customers confidential. It does so mainly to prevent competitors from "stealing" those customers, i.e., from taking advantage of Akamai's sales and marketing efforts and expenditures by targeting businesses that have already been educated by Akamai about the usefulness of buying Internet content delivery services. Akamai spends time, money, and effort to identify and sell prospective customers on the benefits of content delivery. A competitor would have an advantage over Akamai if it could piggyback on Akamai's investments and avoid spending its resources on such marketing and sales efforts by pursuing only those organizations known to have already decided to use content delivery network services.

Like the customer list, the contracts between Akamai and various customers that DOXER provided the UC contained trade secrets. Among other things, each contract specifies the customer's name and contact information, the contract's beginning and end date, the nature of the services being provided, and the fees being charged for each service. That information is all sensitive because knowing it could assist Akamai's competitors in wooing away existing Akamai customers. And by knowing the expiration date of Akamai's contract with a particular customer, a competitor would know the optimum time to make a pitch for that customer's business. By knowing the contract's services and fees, the competitor would know exactly what services and terms

to offer in order to undercut Akamai. (The service fees associated with Akamai contracts are not publicized, nor is the information standardized.)

Akamai protects its confidential business information -- including the information described above -- in a number of ways:

- It requires visitors to its offices to be escorted by Akamai personnel.
- Its employees must present security proximity badges to access Akamai's physical building and offices. Because Akamai generally provides its employees information on a need-to-know basis, the badges do not generally give each employee access to all of Akamai's offices. Rather, they give each employee access to the areas based on the employee's need to access the various departments. For example, employees who are given access to Akamai's general corporate facilities are not typically given access to sensitive engineering areas or other specialized areas.
- Akamai's employees are required to read and sign nondisclosure agreements in which they promise not to disclose the company's confidential business information. They are also provided security awareness training when they begin working for the company, and that training is refreshed annually for all employees. Additional security awareness training is provided for employees with certain sensitive duties. Akamai's information security personnel remind employees of their periodic

security training and track employees' completion.

- Akamai's employee handbook and code of business conduct and ethics also require employees to protect and not disclose confidential proprietary information.
- All Akamai employees are also required to sign an agreement not to compete against Akamai or solicit Akamai's customers for a period after leaving Akamai's employ.
- Akamai labels certain documents as proprietary or confidential to indicate that employees should not release this information outside the company without appropriate need or permission. The contracts that DOXER provided were generally marked as confidential.